

# ALTERNATIVE PROOF OF A TECHNICAL LEMMA FOR THE ANALYSIS OF RANDOM K-XORSAT

GREGORY B. SORKIN

ABSTRACT. Pittel and Sorkin’s “The Satisfiability Threshold for  $k$ -XORSAT” proves a lemma governing a certain function of several variables, from this deriving a corollary that is their main result. This note gives an alternative proof.

## 1. NOTATION AND FACT TO BE PROVED

Pittel and Sorkin’s “The Satisfiability Threshold for  $k$ -XORSAT” includes Lemma 4, governing a certain function of several variables, which it uses to establish Corollary 7, which is essentially their main result. This note’s Lemma 1 and Corollary 2 are “drop-in replacements” for those two results. Its purpose is to offer an alternative to Lemma 4 (page 11) of [PiSo2012] and its proof (pages 14–21 and 24–26).

The proof here borrows liberally from that in [PiSo2012] and a proof sketch suggested earlier by Paul Balister [Ba2012].

The context is a random XORSAT formula with  $n$  variables,  $m$  clauses, and  $k$  variables per clause, where  $m = cn$ ,  $c \in (2/k, 1)$  and  $k > 3$  are fixed,  $n \rightarrow \infty$ , and all  $O(\cdot)$  expressions are with respect to this limit. Also, we have a function  $f$  arising from a truncated Poisson distribution

$$f(x) = \sum_{j \geq 2} \frac{x^j}{j!} = e^x - 1 - x.$$

and we define  $\lambda$  as the unique root of

$$\frac{xf'(x)}{f(x)} = \frac{km}{n} = kc;$$

all details are in [PiSo2012]. Our starting point is inequality [PiSo2012, eq (18)], governing an expression of interest that we will not define here:

$$\begin{aligned} \mathbb{E}[Y_{m,n}^{(\ell)}] &\leq O(1) \sqrt{\frac{\lambda}{z_2}} \binom{m}{\ell} \binom{km}{k\ell}^{-1} \lambda^{km} \\ (1) \quad &\times \frac{1}{z_1^{k\ell} z_2^{k(m-\ell)}} \left( \frac{f(z_2) + e^{z_2}(\cosh z_1 - 1)}{f(\lambda)} \right)^n, \quad \forall z_1, z_2 > 0, \end{aligned}$$

where  $\ell \in \{2, \dots, m\}$ . Observe that

$$f(z_2) + e^{z_2}(\cosh z_1 - 1) = \frac{f(z_1 + z_2) + f(z_2 - z_1)}{2}.$$

Using the Stirling formula for factorials, recalling from [PiSo2012] that  $m = cn$  with  $c \in (2/k, 1)$ , and introducing  $\alpha = \ell/m$ ,  $\bar{\alpha} = 1 - \alpha$ ,  $z_1 = \zeta_1 \lambda$ ,  $z_2 = \zeta_2 \lambda$ , and  $\zeta = (\zeta_1, \zeta_2)$ , we rewrite (1) as

$$(2) \quad \mathbb{E}[Y_{m,n}^{(\ell)}] \leq O(1) \sqrt{\frac{1}{\zeta_2}} \exp[nH_k(\alpha, \zeta; c)], \quad \forall \zeta > 0,$$

where we have used  $\sqrt{k} = O(1)$ , defined

$$(3) \quad H_k(\alpha, \zeta; c) = cH(\alpha) - ck\alpha \ln(\zeta_1/\alpha) - ck\bar{\alpha} \ln(\zeta_2/\bar{\alpha}) \\ + \ln \frac{f(\lambda(\zeta_2 + \zeta_1)) + f(\lambda(\zeta_2 - \zeta_1))}{2f(\lambda)},$$

and where  $H(\alpha)$  is the usual entropy function

$$H(\alpha) := -\alpha \ln \alpha - (1 - \alpha) \ln(1 - \alpha).$$

The main purpose of this note is to prove the following lemma, which we will do in the next section.

**Lemma 1.** *For all  $k \geq 4$ , letting*

$$(4) \quad a_k = ek^{-k/(k-2)},$$

*for all  $c \in (2/k, 1)$ , there exist  $\varepsilon, \zeta_0 > 0$ , such that*

$$(5) \quad (\forall \alpha \in (0, \alpha_k]) (\exists \zeta): H_k(\alpha, \zeta; c) \leq (c\alpha)(\frac{k}{2} - 1) \ln(\alpha/\alpha_k) \text{ and } \zeta_2 > \zeta_0$$

$$(6) \quad (\forall \alpha \in [\alpha_k/3, 1]) (\exists \zeta): H_k(\alpha, \zeta; c) \leq -\varepsilon \text{ and } \zeta_2 > \zeta_0.$$

This will yield the following corollary, very similar to [PiSo2012, Corollary 7] and establishing Pittel and Sorkin's main result.

**Corollary 2.** *For all  $k \geq 4$  and all  $c \in (2/k, 1)$ ,*

$$\mathbb{E}[Y_{m,n}] = \sum_{\ell=2}^m \mathbb{E}[Y_{m,n}^{(\ell)}] = O(m^{-(k-2)}).$$

In the paper's context, the Corollary says that the expected number of nonempty critical row sets tends to 0, by the first moment method so does the probability of any such set, and thus the linear system is solvable, asymptotically almost surely.

*Proof of Corollary.* Letting  $\ell_k = \alpha_k m = \Theta(n)$ , for  $\ell \leq \ell_k/2$ , recalling that  $\alpha cn = \alpha m = \ell$ , (2) and (5) give

$$\mathbb{E}[Y_{m,n}^{(\ell)}] = O(1) \exp[(\frac{k}{2} - 1)\ell \ln(\ell/\ell_k)].$$

By convexity of  $\ell \ln(\ell/\ell_k)$ , for  $\ell \in [2, \ell_k/2]$ ,

$$\begin{aligned} \ell \ln(\ell/\ell_k) &\leq 2 \ln(2/\ell_k) + \frac{\ell - 2}{\ell_k/2 - 2} ((\ell_k/2) \ln(1/2) - 2 \ln(2/\ell_k)) \\ &= 2 \ln(2/\ell_k) + (\ell - 2)(-\ln 2 + o(1)), \end{aligned}$$

using that  $\ell_k = \Theta(n)$ . Thus,

$$\begin{aligned} \mathbb{E}[Y_{m,n}^{(\ell)}] &\leq O(1) \exp\left(\left(\frac{k}{2} - 1\right)2[\ln(2/\ell_k) - 0.6(\ell - 2)]\right) \\ &= O(1) m^{-(k-2)} \exp(-0.6(\ell - 2)), \end{aligned}$$

where we have hidden a  $(2/\alpha_k)^{k-2}$  in the  $O(1)$ . Then,

$$\sum_{\ell=2}^{\lfloor (\alpha_k/2)m \rfloor} \mathbb{E}[Y_{m,n}^{(\ell)}] = O(1) (m^{-(k-2)}).$$

For  $\ell > (\alpha_k/2)m$ , by (6),

$$\mathbb{E}[Y_{m,n}^{(\ell)}] = O(1) \exp(-\varepsilon n),$$

giving

$$\sum_{\ell=\lceil (\alpha_k/2)m \rceil}^m \mathbb{E}[Y_{m,n}^{(\ell)}] = \exp(-\Omega(n)).$$

Adding the two partial sums yields Corollary 2.  $\square$

## 2. PROOF OF LEMMA 1

Motivation for the values of  $\zeta_1$  and  $\zeta_2$  used to control  $H_k(\alpha, \zeta; c)$  is given in [PiSo2012]. Lemma 1 is proved by Claims 3, 4, 5 and 6, respectively treating  $\alpha$  in the four ranges  $(0, 0.99\alpha_k]$ ,  $[0.99\alpha_k, 0.2743]$ ,  $(0.2743, 1/2]$ , and  $(1/2, 1)$ . Recall the notation  $\bar{\alpha} = 1 - \alpha$  and  $\zeta = (\zeta_1, \zeta_2)$ .

**Claim 3.** *For all  $k \geq 3$  and all  $c \in (2/k, 1)$ , for all  $\alpha \in (0, \alpha_k)$ , taking*

$$(7) \quad \zeta_1 = (ck)^{-1/2} \alpha^{1/2}, \quad \zeta_2 = \bar{\alpha},$$

*yields  $H_k(\alpha, \zeta; c) \leq (c\alpha)(\frac{k}{2} - 1) \ln(\alpha/\alpha_k)$ .*

*Also, for all  $k \geq 3$  and all  $c \in (2/k, 1)$ , there exists  $\varepsilon > 0$  such that for all  $\alpha \in [\alpha_k/3, 0.99\alpha_k]$ , the same  $\zeta$  yields  $H_k(\alpha, \zeta; c) < -\varepsilon$  with  $\zeta_2 = \Theta(1)$ .*

*Proof.* The issue in this range of  $\alpha$  is to control the final logarithmic term of  $H_k(\alpha, \zeta; c)$  when the two summands within the logarithm are nearly equal. Note that  $\ln f(x)$  is concave on either side of 0, as

$$[\ln f(x)]'' = \frac{e^x(1 - x - e^{-x})}{f^2(x)} < 0.$$

Since  $\frac{d}{d\Delta} \ln f(\lambda(1 + \Delta)) = \frac{\lambda f'(\lambda)}{f(\lambda)}$ , if  $\lambda$  and  $\lambda(1 + \Delta)$  are on the same side of 0 (if  $1 + \Delta \geq 0$ ) then concavity gives  $\ln f(\lambda(1 + \Delta)) \leq \ln f(\lambda) + \Delta \frac{\lambda f'(\lambda)}{f(\lambda)}$ . Or,

with  $\zeta = 1 + \Delta$ , if  $\zeta \geq 0$  then

$$(8) \quad \frac{f(\lambda\zeta)}{f(\lambda)} \leq \exp\left((\zeta - 1)\frac{\lambda f'(\lambda)}{f(\lambda)}\right) = \exp((\zeta - 1)ck),$$

recalling that  $\lambda f'(\lambda)/f(\lambda) = ck$ . It is easily checked that (4) gives  $\alpha_k < 0.2$  for  $\zeta_2 > 0.8$  and (7) then gives  $\zeta_1 < 0.4$ , so  $\zeta_2 + \zeta_1 \geq 0$  and  $\zeta_2 - \zeta_1 \geq 0$ . Thus for the final term of  $H_k(\alpha, \zeta; c)$ , we have

$$\begin{aligned} & \ln \frac{f(\lambda(\zeta_2 + \zeta_1)) + f(\lambda(\zeta_2 - \zeta_1))}{2f(\lambda)} \\ & \leq \ln \left( \frac{\exp(ck(\zeta_2 + \zeta_1 - 1))}{2} + \frac{\exp(ck(\zeta_2 - \zeta_1 - 1))}{2} \right) \\ & = \ln \left( \exp(ck(\zeta_2 - 1)) \left[ \frac{\exp(ck\zeta_1) + \exp(-ck\zeta_1)}{2} \right] \right) \\ & = ck(\zeta_2 - 1) + \ln \cosh(ck\zeta_1) \\ & \leq ck(\zeta_2 - 1) + (ck\zeta_1)^2/2, \end{aligned}$$

using the general fact that  $\ln \cosh x \leq x^2/2$ . Now also using  $-\bar{\alpha} \ln \bar{\alpha} \leq a$  for all  $\bar{\alpha} \in (0, 1)$ , from (7),

$$\begin{aligned} H_k(\alpha, \zeta; c) & \leq -c\alpha \ln \alpha + c\alpha - ck\alpha \ln(ck\alpha)^{-1/2} - 0 + ck(-\alpha) + \sqrt{ck\alpha}^2/2 \\ & \leq c\alpha[(\frac{k}{2} - 1) \ln \alpha + (1 - \frac{k}{2}) + \frac{1}{2}k \ln(ck)] \\ & = (c\alpha)(\frac{k}{2} - 1) \ln[\alpha \frac{1}{e}(ck)^{k/(k-2)}]. \end{aligned}$$

Pessimistically taking  $c = 1$  within the logarithm and recalling (4),

$$(9) \quad H_k(\alpha, \zeta; c) \leq (c\alpha)(\frac{k}{2} - 1) \ln(\alpha/\alpha_k).$$

This proves the first part of the claim.

Clearly, for all  $\alpha \in (0, \alpha_k)$  the logarithm in (9) is negative, so over any properly contained sub-interval,  $H_k(\alpha, \zeta; c)$  is bounded below 0, i.e.,  $h_k(\alpha; c) \leq -\varepsilon$  for some  $\varepsilon > 0$ . From (7) it is also immediate that  $\zeta_2$  is bounded away from 0. This establishes the second part of the claim.  $\square$

**Claim 4.** For all  $k \geq 4$  and all  $c \in (2/k, 1)$ , there exists  $\varepsilon > 0$  such that for all  $\alpha \in (0.99\alpha_k, 0.2743]$ , taking  $\zeta_1 = \alpha$ ,  $\zeta_2 = \bar{\alpha}$  yields  $H_k(\alpha, \zeta; c) < -\varepsilon$  and  $\zeta_2 = \Theta(1)$ .

*Proof.* That  $\zeta_2 = \Theta(1)$  is immediate. Now,

$$\begin{aligned} (10) \quad H_k(\alpha, \zeta; c) & = cH(\alpha) + \ln \left( \frac{1}{2} + \frac{1}{2} \frac{f(\lambda(1 - 2\alpha))}{f(\lambda)} \right) \\ & \leq cH(\alpha) + \ln \left( \frac{1}{2} + \frac{1}{2} \exp(-2ck\alpha) \right) \quad (\text{by (8) and } 1 - 2\alpha > 0) \\ & \leq c[H(\alpha) + \ln \left( \frac{1}{2} + \frac{1}{2} \exp(-2k\alpha) \right)], \end{aligned}$$

the last step following from concavity of  $\ln(\frac{1}{2} + \frac{1}{2} \exp(-2ck\alpha)) =: g(c)$  as a function of  $c$ . The application of concavity is simply  $g(c) \leq (1 - c)g(0) +$

$cg(1) = cg(1)$  using  $g(0) = 0$ . The proof of concavity is that, with  $L = 2k\alpha$ ,

$$\frac{d^2g}{dc^2} = c^2 \left[ \frac{\exp(-cL)}{1 + \exp(-cL)} - \left( \frac{\exp(-cL)}{1 + \exp(-cL)} \right)^2 \right] \geq 0,$$

the inequality following from negativity of the exponent's argument, so that the fraction lies between 0 and 1/2.

From (10), it suffices to prove that

$$s_k(\alpha) := H(\alpha) + \ln\left(\frac{1}{2} + \frac{1}{2}\exp(-2k\alpha)\right)$$

is negative for  $\alpha \in [0.99\alpha_k, 0.2743]$ . For a fixed  $k$  this can be confirmed by interval arithmetic. It suffices to cover the interval with sub-intervals  $[\alpha', \alpha'']$  for each of which  $H(\alpha'') + \ln(\frac{1}{2} + \frac{1}{2}\exp(-2k\alpha')) < 0$ : the arguments  $\alpha''$  and  $\alpha'$  pessimistically maximize the first and second terms independently. For numerical security, we will choose intervals establishing that  $s_k(\alpha) < -0.0001$ .

For  $k = 4$ ,  $0.1681 < 0.99\alpha_k$  and 49 intervals suffice to cover  $[0.1681, 0.2743]$  and show that  $s_k(\alpha) < -0.0001$ . For  $k = 5$ ,  $0.1839 < 0.99\alpha_k$ , and 2 intervals suffice:  $[0.1839, 0.2291]$  and  $[0.2291, 0.2743]$ . For  $k = 6$  a single interval would suffice. However, noting that  $\frac{1}{k} < 0.99\alpha_k$ , we instead establish that  $s_k(\alpha) < -0.0001$  over the larger interval  $[\frac{1}{k}, 0.2743]$ ; for this, the two intervals  $[0.1666, 0.2204]$ ,  $[0.2204, 0.2743]$  suffice.

For  $k \geq 6$ ,  $\frac{1}{k} < 0.99\alpha_k$ . (Check that  $\ln k - \frac{k-2}{2} \ln(0.99e) < 0$  at  $k = 6$  and has negative derivative for  $k \geq 6$ .) We now prove by induction on  $k$  that  $s_k(\alpha) < 0$  over  $\alpha \in [\frac{1}{k}, 0.2743]$ , for  $k \geq 6$ . We have already established the base case. Since  $s_k(\alpha)$  is monotone decreasing in  $k$ ,  $s_k(\alpha) \leq s_{k-1}(\alpha) < 0$  for  $\alpha \in [\frac{1}{k-1}, 0.2743]$ , by the inductive hypothesis, so we need only show that  $s_k(\alpha) < 0$  for  $\alpha \in [\frac{1}{k}, \frac{1}{k-1}]$ . Over this interval,  $H(\alpha) \leq H(\frac{1}{k-1}) \leq H(\frac{1}{6}) < 0.451$ , while the other term of  $s_k(\alpha)$  is decreasing in  $k\alpha$ , and  $k\alpha \geq 1$ , so  $\ln(\frac{1}{2} + \frac{1}{2}\exp(-2k\alpha)) \leq \ln(\frac{1}{2} + \frac{1}{2}\exp(-2)) < -0.566$ ; summing the two terms proves that  $s_k(\alpha) < 0$ .  $\square$

**Claim 5.** *For all  $k \geq 4$  and all  $c \in (2/k, 1)$ , there exists  $\varepsilon > 0$  such that for all  $\alpha \in (0.2743, 1/2]$ , taking  $\zeta_1 = \alpha$ ,  $\zeta_2 = \bar{\alpha}$  yields  $H_k(\alpha, \zeta; c) < -\varepsilon$  and  $\zeta_2 = \Theta(1)$ .*

*Proof.* Again,  $\zeta_2 = \Theta(1)$  is immediate. In this case, with  $\alpha$  relatively close to 1/2, the key is to govern the term  $f((1-2\alpha)\lambda)/f(\lambda)$ . Motivated by the small- $\lambda$  asymptotic equality  $f(\lambda) \sim \frac{1}{2}\lambda^2$ , we will show that

$$R(\lambda, x) := \frac{f(x\lambda)}{x^2 f(\lambda)} \leq q,$$

where we may choose  $q = 1$  for any  $x \in (0, 1)$  and  $\lambda > 0$ , and smaller values of  $q$  for restricted ranges of  $x$  and  $\lambda$ .

To establish this, we first show that  $R(\lambda, x)$  is increasing with  $x$ .

$$\frac{d}{dx} \ln(R(\lambda, x)) = \frac{\lambda f'(\lambda x)}{f(\lambda x)} - \frac{2}{x} = \frac{1}{xf(s)} (sf'(s) - 2f(s)),$$

where we define  $s := \lambda x$ . Using  $e^s > 1 + s$ ,

$$\begin{aligned} sf'(s) - 2f(s) &= s(e^s - 1) - 2(e^s - s - 1) \\ &= (s - 2)e^s + s + 2 > (s - 2)(1 + s) + s + 2 = s^2 > 0, \end{aligned}$$

establishing that  $\frac{d}{dx} \ln(R(\lambda, x)) > 0$  and thus that  $R(\lambda, x)$  is increasing in  $x$ .

We next show that  $R(\lambda, x)$  is decreasing with  $\lambda$ .

$$\frac{d}{d\lambda} \ln(R(\lambda, x)) = -\frac{f'(\lambda)}{f(\lambda)} + \frac{xf'(\lambda x)}{f(\lambda x)},$$

and we wish to show that this is  $\leq 0$ . It is easy to check that it is equal to 0 in the limit  $x \rightarrow 1$ , so it suffices to check that it is increasing with respect to  $x$  for  $x > 0$ . Since the first term is constant and  $\lambda$  is constant, this is equivalent to  $\lambda x f'(\lambda x)/f(\lambda x)$  being increasing with respect to  $\lambda x$ , an easy fact given as [PiSo2012, Note 1].

We have now established that if  $f(\lambda_0 x_0)/(x_0^2 f(\lambda_0)) = q$ , then for all  $\lambda > \lambda_0$  and all  $x \in (0, x_0]$ ,  $f(\lambda x)/f(\lambda) \leq qx^2$ . In particular,  $f(\lambda x)/f(\lambda) \leq x^2$ , for all  $\lambda > 0$  and all  $x \in (0, 1]$ , because the limit  $\lambda_0 \rightarrow 0$ ,  $x_0 \rightarrow 1$  gives  $q = 1$ .

We also use that

$$H(\tfrac{1}{2} - x) \leq \ln \frac{2}{2x^2 + 1}.$$

This can be verified by checking that  $H(\tfrac{1}{2} - x) - \ln \left( \frac{2}{2x^2 + 1} \right)$  and its first derivative are both 0 at  $x = 0$ , while the second derivative is  $-\frac{16x^2}{(2x^2 + 1)^2} - \frac{4}{1 - 4x^2} + \frac{4}{1 + 2x^2} < 0$  for  $x \in (0, 1/2)$ .

Recalling that Claim 4 covered  $\alpha \in (1/k, \alpha_0]$  with  $\alpha_0 = 0.2743$ , we need only be concerned with  $x \in (0, x_0)$ ,  $x_0 = \tfrac{1}{2} - \alpha_0 = 0.2257$ . We treat this with two cases.

For  $\lambda \geq \lambda_0 = 2.7694$  and  $x \in (0, x_0)$ ,  $f(2\lambda x)/f(\lambda) < 0.4999$ . Thus

$$\begin{aligned} H_k(\alpha, \zeta; c) &= cH(\tfrac{1}{2} - x) + \ln \left( \tfrac{1}{2} + \tfrac{1}{2} \cdot \frac{f(2\lambda x)}{f(\lambda)} \right) \\ &< \ln \left( \frac{2}{2x^2 + 1} \right) + \ln \left( \tfrac{1}{2} + \tfrac{1}{2} \cdot 0.4999(2x)^2 \right) \\ &= \ln \left( \frac{1.9996x^2 + 1}{2x^2 + 1} \right) \\ &< 0. \end{aligned}$$

For  $\lambda < \lambda_0$ , we have  $ck < 3.3992$ , so using  $ck/k = c$  and  $k \geq 4$ ,

$$\begin{aligned} H_k(\alpha, \zeta; c) &< \frac{3.3992}{4} H\left(\frac{1}{2} - x\right) + \ln\left(\frac{1}{2} + \frac{1}{2} \cdot 1 \cdot (2x)^2\right) \\ &< \frac{3.3992}{4} \ln\left(\frac{2}{2x^2 + 1}\right) + \ln\left(\frac{4x^2 + 1}{2}\right), \\ &< 0 \quad \text{for } x \in [0, x_0]. \end{aligned}$$

The final statement can be checked by verifying that the previous expression has nonnegative derivative and, at  $x = x_0$ , is  $< -0.0011$ .  $\square$

**Claim 6.** *For all  $k \geq 4$  and all  $c \in (2/k, 1)$ , there exists  $\varepsilon > 0$  such that for all  $\alpha \in (1/2, 1]$  there exists  $\zeta$ , with  $\zeta_2 = \Theta(1)$ , for which  $H_k(\alpha, \zeta; c) < -\varepsilon$ .*

*Proof.* Since  $f(x) > f(-x)$  for  $x > 0$ , and  $\lambda = \lambda(kc) > 0$ ,

$$H_k(1, (1, 0); c) = \ln \frac{f(\lambda) + f(-\lambda)}{2f(\lambda)} < 0.$$

By continuity of  $H_k(\alpha, (1 - \zeta_2, \zeta_2); c)$  in  $\alpha$  and  $\zeta_2$ , for  $\delta = \delta(c, k) > 0$  sufficiently small,

$$\sup_{\alpha \in [1-\delta, 1]} H_k(\alpha, (1 - \delta, \delta); c) < 0.$$

So, for  $\alpha \geq 1 - \delta$ , taking  $\zeta = (\zeta_1, \zeta_2) = (1 - \delta, \delta)$  yields the claim.

For  $\alpha \in (\frac{1}{2}, 1 - \delta]$ , let  $\zeta(\bar{\alpha}; c)$  denote the values given by Claims 3–5, and here (noting the coordinate swap), set  $(\zeta_2, \zeta_1) := \zeta(\bar{\alpha}; c)$ . Immediately,

$$H_k(\alpha, (\zeta_1, \zeta_2); c) < H_k(1 - \alpha, (\zeta_2, \zeta_1); c) = H_k(\bar{\alpha}, \zeta; c) < 0,$$

the first inequality by inspection of the symmetries of (3) and  $\zeta_2 \leq \zeta_1$  (checking that in Claims 3–5,  $\zeta_1 \leq \zeta_2$ ), and the second inequality immediate from Claims 3–5. Finally,  $\zeta_2 = \Theta(1)$  because  $\zeta_2$  here for  $\alpha \in [\frac{1}{2}, 1 - \delta]$  is equal to an earlier claim's  $\zeta_1$  for  $\alpha \in [\delta, \frac{1}{2}]$ , variously of order  $\Theta(\alpha^{1/2})$  or  $\Theta(\alpha)$ , and in either case bounded away from 0 since  $\alpha \geq \delta$ .  $\square$

This completes the proof of Lemma 1 and thus this note.

## REFERENCES

- [PiSo2012] B. Pittel and G.B. Sorkin, “The Satisfiability Threshold for  $k$ -XORSAT”, manuscript, June 2012. (Uploaded as <http://arxiv.org/pdf/1212.1905.pdf> Dec 2012.)
- [Ba2012] P. Balister, personal communication, Apr 2012.

(Gregory B. Sorkin) DEPARTMENT OF MANAGEMENT, LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE, HOUGHTON STREET, LONDON WC2A 2AE

*E-mail address:* [g.b.sorkin@lse.ac.uk](mailto:g.b.sorkin@lse.ac.uk)